Department of Homeland Security Daily Open Source Infrastructure Report for 29 September 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The San Jose Mercury News reports that San Francisco International Airport is the first in the nation set to accept new passports embedded with computer chips that contain a traveler's photo and data. (See item 10)
- The San Diego Union−Tribune reports that U.S. authorities determined Wednesday, September 27, that a tunnel under construction on the Mexican side of the San Ysidro border crossing extended 15 feet into U.S. territory. (See item 11)
- US−CERT released Technical Cyber Security Alert TA06−270A: Microsoft Internet Explorer WebViewFolderIcon ActiveX vulnerability. (See item 29)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *September 28, Associated Press* — **Experts predict lower winter gas costs.** Natural gas producers predicted Thursday, September 28, that consumers will see lower prices this winter because there's plenty of natural gas already in storage and more is being produced. The Natural Gas Supply Association (NGSA) said in a report that there are record supplies of the fuel in storage, well above normal levels as the winter heating season approaches. It said that

wholesale prices already have been declining significantly. "For the first time in four years we're seeing downward pressure on prices," said Chris Conway of ConocoPhillips. A year ago, as the industry faced major losses of supply because of Hurricane Katrina, wholesale prices going into the winter ranged from around $12 per thousand cubic feet. Recently, the prices dipped below $4.50 per thousand cubic feet at the wholesale level. Conway said that overall, natural gas production this year "will be substantially higher" than in 2005, as the industry steadily recovered from the hurricane a year ago and stepped up onshore production.
NGSA press release: http://www.ngsa.org/newsletter/pdfs/Final_PressReleasePDF.pd f
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/09 /28/AR2006092800689.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *September 28, King County Journal (WA)* — **Gas line break in Washington prompts voluntary evacuations.** At least 100 people voluntarily evacuated buildings in downtown Bellevue, WA, on Wednesday, September 27, after a natural gas line was accidentally broken by construction equipment as workers performed routine maintenance in the area. Puget Sound Energy (PSE) spokesperson David Reid, said the leak was caused when workers with Pilchuck Contractors, a subcontractor that performs work on PSE's natural gas lines, tried to install a corrosion protection device on a steel line. The equipment they were using inadvertently struck a 2−inch plastic main line, causing the leak.
Source: http://www.kingcountyjournal.com/apps/pbcs.dll/article?AID=/ 20060928/NEWS/609280316

[Return to top]

Defense Industrial Base Sector

3. *October 01, National Defense* — **Combat vehicle designs seek increased utility in multiple roles.** Combat vehicles are being developed to keep pace with soldiers' evolving battlefield roles. Those vehicles increasingly are wheeled, armored and modular, and are incorporating designs that cater to the requirements of ground troops. Many of them will provide soldiers with energy sources, information and weapons they will need to fight, while giving them added protection. The prevalence of such vehicles at one of the largest ground warfare expositions reveals a trend in how armies are choosing to insert their troops into hot spots. Light armored vehicles have become the preferred mode of infantry transport into battlefields that increasingly encompass urban landscapes and a wider range of operations. The Boxer, an eight−wheeled, 25−ton armored vehicle developed by a Munich, Germany−based consortium, resembles the U.S. Army's Stryker combat vehicle with one major exception: Its interchangeable mission module design allows any Boxer platform to switch functions, from armored personnel carrier to command post to ambulance to cargo carrier.
Source: http://www.nationaldefensemagazine.org/issues/2006/October/C ombatvehicle.htm

4.

September 28, Aviation Now — **Defense supplemental a boon to several companies, analyst says.** The "usual" list of companies stand to benefit from the pending, initial fiscal 2007 defense supplemental account, including General Dynamics, Northrop Grumman, ITT, ATK, Oshkosh and Armor Holdings among others, according to a UBS analyst. Programs receiving the largest funding out of the $70 billion supplemental include Humvees, M1 Abrams and the Army's families of medium and heavy tactical vehicles. The latest supplemental funds include $19.8 billion for procurement −− a higher percentage toward procurement than recent prior supplementals, UBS analyst David Strauss noted. This follows the second FY '06 supplemental worth $115 billion that included $25 billion for procurement, expanding a pattern of growing procurement based in off−budget, noncapped accounts. Another FY '07 supplemental request is expected from the White House, possibly early next year, and would be worth tens of billion of dollars more.
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/SUPP09286.xml

[Return to top]

Banking and Finance Sector

5. *September 28, Register (UK)* — **UK banking Websites' security rife with vulnerabilities.** Several major UK bank Websites are subject to security flaws that make it easier for phishing scammers to craft more convincing scams, according to a study by Heise Security. Friday, September 22, Heise published a number of demos to show how phishing scammers might be able to overlay the websites of NatWest, Cahoot, Bank of Scotland, Bank of Ireland, First Direct, and Link with rogue frames, potentially served from Websites controlled by scammers. Cross site scripting attacks against the Websites of USB and the Bank of England's site were also demonstrated. Frame spoofing attacks can be thwarted providing users are using up to date browser software, but the cross−site scripting attacks it demonstrated can't be addressed by client−side security updates, according to Heise. Both types of attacks require a modicum of skill to carry out, but are far from difficult. A number of banks −− including HSBC, Barclays and the Halifax −− were not vulnerable to Heise Security's tests. HSBC, for example, uses JavaScript code to check the integrity of the frameset, an approach that thwarts frame spoofing even if a surfer is using out−of−date browser software.
Source: http://www.channelregister.co.uk/2006/09/28/uk_banking_secur ity_study/

6. *September 28, Washington Post* — **ID thieves turn sights on smaller e−businesses.** While public attention has remain fixed on a series of high−profile data losses or database breaches at federal government agencies, large corporations, and universities, experts who study financial fraud say hackers increasingly are targeting small, commercial Websites. In some cases, criminals are able to gain real−time access to the sites' transaction information, allowing them to steal valid credit card numbers and quickly charge large numbers of fraudulent purchases. Small e−businesses offer fewer total victims, but they often present a softer target, either due to flaws in the software merchants use to process online orders or an over reliance on outsourced Website security. Dan Clements of CardCops.com, a fraud prevention service that monitors underground chat rooms where criminals trade in stolen credit cards and information used to commit identity theft, said many smaller online merchants use generic shopping cart software that they fail to maintain with the latest software security patches. Nearly 80 percent of all

software vulnerabilities discovered in the first six months of 2006 involved Web−based applications produced by hundreds of different software vendors, according to a report released Monday, September 25, by Symantec Corp.
Symantec Report: http://www.symantec.com/specprog/threatreport/ent−whitepaper_symantec_internet_security_threat_report_x_09_2006.en−us.pd f
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/09/28/AR2006092800333_pf.html

7. *September 28, Associated Press* — **Thieves take North Carolina DMV computer with personal info.** Thieves have taken a computer containing the sensitive personal information of thousands of North Carolina motorists, the state's Division of Motor Vehicles (DMV) says. The DMV has mailed notifications to 16,000 drivers that someone took the computer from the agency's Louisburg office earlier this month. The computer contained personal information −− including Social Security numbers, birth dates, and drivers license numbers −− for some motorists who received new licenses between March 2005 and September 10. Most vulnerable motorists are residents of Franklin County, where Louisburg is located, said DMV spokesperson Marge Howell. Howell said the personal information is not easily accessible and there is no evidence that it has been used for identity theft.
Source: http://citizen−times.com/apps/pbcs.dll/article?AID=200660928 001

8. *September 28, Capitol Media Services (AZ)* — **New Arizona law mandates that businesses destroy records with personal data.** Companies must start shredding or otherwise destroying records with personal customer and employee information when they've finished with the records. A law that takes effect October 1 in Arizona makes it a crime for businesses to knowingly dispose of paper records if identifying information can be read. The Identity Theft Data Clearinghouse, administered by the Federal Trade Commission, reported more than 9,300 complaints of identity theft filed last year. The new requires that records must be destroyed, or at least the information obliterated, if it contains at least an individual's first initial and last name if it also contains other identifying numbers. That list includes Social Security, credit and debit cards, bank accounts, and driver's licenses. The law exempts entities that must comply with federal laws, including financial institutions and health care providers. It also is crafted to apply solely to paper records, not electronic files.
Source: http://www.azcentral.com/abgnews/articles/0928abg−record0928 .html

9. *September 27, Tallahassee Democrat (FL)* — **Farmers and Merchants Bank shuts down e−mail scam.** Farmers and Merchants Bank (FMB) officials quickly shut down an e−mail scam Tuesday, September 26, that purported to be coming from the bank's Monticello, FL, headquarters. No customers' private information was compromised by the scam, a bank official said. An official−looking e−mail offered FMB customers $100 for answering a quick, five−question online survey. The e−mail offer claimed the survey would not ask for sensitive information, but if a customer accessed the e−mail link to the survey, they found that claim not to be true, said Mike Sims of FMB. The bank quickly acted to shut down the e−mail and Weblink Tuesday morning shortly after the bank began receiving reports of the scam's existence, Sims said.
Source: http://www.tallahassee.com/apps/pbcs.dll/article?AID=/20060927/BUSINESS/609270312/1003

[Return to top]

Transportation and Border Security Sector

10. *September 28, San Jose Mercury News (CA)* — **San Francisco airport set for new passports.** San Francisco International Airport is the first in the nation set to accept new passports embedded with computer chips that contain a traveler's photo and data, federal officials announced Wednesday, September 27. The airport, which federal officials said was a test site for the new passports, is one of 33 that will get the chip−reading machines, which are being put in place over the next few weeks in order to meet an October 26 deadline mandated by Congress. Starting on that date, 27 ally countries whose citizens don't need visas for short−term business and tourist travel to the U.S. will be required to issue passports that include the chips. The U.S. has already started to issue such passports. The chip will hold a traveler's photograph and the biographical information printed on his passport. It will also have the capability to hold digital fingerprints and iris scans.
Source: http://www.mercurynews.com/mld/mercurynews/news/local/156278 93.htm

11. *September 28, San Diego Union−Tribune* — **Tunnel extended into U.S., authorities say; five detained.** U.S. authorities determined Wednesday, September 27, that a tunnel under construction on the Mexican side of the San Ysidro border crossing had actually extended into the U.S. The tunnel crossed about 15 feet into U.S. territory, though it had no exit on the U.S. side, said Lauren Mack, a spokesperson with Immigration and Customs Enforcement. Mexican authorities detained five people −− including two Mexican Customs inspectors −− suspected of being involved in the construction. The tunnel was found Tuesday, September 26. U.S. authorities found digging equipment inside the four−foot−by−four−foot tunnel, which had been reinforced with wood and plastic, Mack said. Though it wasn't as sophisticated as other tunnels found along the border, the find was notable because it implicates members of Mexican Customs. The tunnel, like four others found over the past year in the same general area, originated in a gated junkyard that the federal agency uses. Tunnels are typically used to smuggle people and drugs. U.S. and Mexican authorities initially thought the tunnel was restricted to the Mexican side. Wednesday, U.S. investigators found it stretched a total of 86 feet, though most of it was in Mexico, Mack said.
Source: http://www.signonsandiego.com/news/mexico/tijuana/20060928−9999−6m28tunnel.html

12. *September 27, Associated Press* — **Men questioned after confrontation on flight.** Federal agents questioned two airline passengers Wednesday, September 27, after a dispute that began when a man sprayed the person sitting next to him with perfume, authorities said. The two men, who were not arrested, were aboard an American Airlines flight from Lima, Peru, to Miami when the confrontation took place, Miami FBI spokesperson Judy Orihuela said. Before the flight, the older man left his assigned seat and laid down in the aisle. He also asked for a glass of water and poured it on his head, Orihuela said. The older man, a 56−year−old Japanese national, then sat in a seat beside a jockey in his 20s, from Louisville, KY. About two hours into the flight, the older man sprayed the jockey with perfume, Orihuela said. The younger man alerted the flight crew, and he and the older man were separated. The plane landed and the two men were questioned, but not arrested, Orihuela said.

Source: http://www.bradenton.com/mld/bradenton/news/breaking_news/15 622447.htm

13. *September 27, Reuters* — **European Union states back limits on liquids aboard planes.** The European Union (EU) moved closer to adopting new, uniform rules on airline security Wednesday, September 27, after aviation experts backed proposals to limit the amount of liquids passengers may take aboard planes. Officials from the EU's 25 member states supported rules allowing passengers to carry on toiletry items such as toothpaste, contact lens solution and perfume but not large drink containers, except those purchased after security checks. Security measures were tightened after authorities in London said in August they had foiled a plot to bomb flights bound for the United States. But different standards throughout Europe led to calls for greater consistency among EU nations. Under the new rules, which would likely come into effect by early November, passengers would be allowed to bring on one re−sealable plastic bag that was "a maximum size of one liter" in which liquid items could be stored. Liquids would have to fit into containers that were 100 ml or smaller, and passengers would be required to present the bag when going through security checkpoints.
Source: http://today.reuters.com/news/articlenews.aspx?type=worldNews&storyID=2006−09−27T192224Z_01_L27500114_RTRUKOC_0_US−AIRLINES−EU−SECURITY.xml&archived=False

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

14. *September 28, Associated Press* — **Japan's farm ministry confirms country's 29th case of mad cow disease.** Japan's Agriculture Ministry said Thursday, September 28, that it had confirmed that a cow from northern Japan had mad cow disease. Tests on the six year−old dairy cow performed at the National Institute of Animal Health confirmed that the cow, which died at a ranch on Japan's northernmost island of Hokkaido, was infected with the fatal illness. Japan has now confirmed 29 animals infected with the fatal illness −− known formally as bovine spongiform encephalopathy −− since the first case in Japan was defected in 2001.
Source: http://www.iht.com/articles/ap/2006/09/28/asia/AS_GEN_Japan_Mad_Cow.php

15. *September 27, Stop Soybean Rust News* — **Rust in Georgia commercial fields; new Louisiana parish has rust.** The first soybean rust in this season's commercial soybeans in Georgia was found in two Washington County fields Tuesday, September 26. This 12th positive Georgia county this year. On Wednesday, September 27, rust was found in Pointe Coupee Parish, LA. The total U.S. count in 2006 today is 72 rust−positive counties and parishes in eight states: Alabama 5; Florida 13; Georgia 12; Louisiana 17; Mississippi two; North Carolina two; South Carolina 16; Texas three.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=966

16. *September 27, Dow Jones* — **Analyst: Animal production vulnerable to attack.** U.S. livestock production is inherently susceptible to a terrorist attack, due to the way it is structured said a political scientist for a non−profit think tank. "The concentrated nature of modern farming practices and the close geographic distribution of livestock production in the U.S. makes it vulnerable," said Peter Chalk, senior political scientist for the RAND Corp., at the International Symposium on Agroterrorism Tuesday, September 26. There also is a widespread lack of security and surveillance in place at production facilities, he said. Many simple items like locks and gates are lacking. Cattle also travel long distances during their lifetimes. It was estimated that a pound of meat travels 1,000 miles before it is consumed, he said, and cattle travel hundreds of miles, crossing many state borders, before they reach slaughter weight. The U.S. also has an inefficient disease−reporting system, as many illnesses go unreported, he said. Also, veterinarians are not trained to look for foreign animal diseases, Chalk said.
Source: http://www.cattlenetwork.com/content.asp?contentid=71609

[Return to top]

Food Sector

17. *September 28, Agence France−Presse* — **Norway withdraws U.S. rice products.** Norway has withdrawn rice products from thousands of stores across the country after traces of a banned genetically modified substance were found in rice imported from the U.S., a leading Norwegian rice supplier said. "We found traces of genetically modified rice so we decided immediately to recall the products," Rieber and Soen spokesperson Kjell Svarstad told Thursday, September 28. It was not known which specific strain of genetically modified rice had been imported. The European Union last week announced it would increase its controls on imports of U.S. long−grain rice after banned strains were discovered on the European market despite being certified as laboratory tested. While Norway is not a member of the EU, the Scandinavian country follows strict regulations on the import of genetically modified food stuffs in line with the 25−member bloc.
Source: http://news.yahoo.com/s/afp/20060928/hl_afp/norwayusbiotechgmo_060928122556;_ylt=AsTCR4GqcMaVMp4zo3PudKGJOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

18. *September 28, Reuters* — **Japan imports of U.S. beef slump after ban lifted.** Japanese imports of U.S. beef totaled only 105 tons in August, the first full month of shipments since Tokyo reopened the market to meat from the U.S., government data showed on Thursday, September 28. That figure marks a plunge from the 22,000−25,000 tons of U.S. beef that industry officials say Japan was importing each month in 2003 before it imposed a ban following the discovery of a case of mad−cow disease in the U.S. Industry officials have said that U.S. beef will only make a gradual return to the Japanese market partly due to the lack of sufficient volumes of meat that meets Tokyo's requirements. Philip Seng, president of the U.S. Meat Export Federation, said on September 20 that Japan's purchase of U.S. beef will likely be a modest 15,000 tons this year. Japan was once the top importer of U.S. beef, buying 240,000 tons valued at $1.4 billion in 2003. That accounted for nearly 30 percent of total beef supplies in Japan. Tokyo agreed to resume imports of U.S. beef in late July on condition that the meat only comes from cattle aged up to 20 months. All specified risk material must also be eliminated.

Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/09/28/AR2006092800140.html

19. *September 27, U.S. Department of Agriculture* — **Food safety education conference offers preview of new food safety campaign.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns addressed food safety educators, public health officials and medical professionals at an innovative national food safety conference Wednesday, September 27, in Denver, CO. "This conference helps educate doctors, nurses and health officials about those who are most at risk to food borne illness, including young children, older adults, pregnant women, and people with weakened immune systems," said Johanns. "It's my hope USDA will reach as many Americans as possible about the importance of food safety."
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/09/0382.xml

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

20. *September 28, Reuters* — **Indonesia man dies of bird flu, cluster case unlikely.** A 20−year−old Indonesian man who health officials thought had been part of a family cluster of bird flu cases died of the disease on Thursday, September 28, a hospital official said. The man's 25−year−old brother died on Sunday, September 24, after displaying bird flu symptoms but there has been no positive confirmation he had the disease because no samples were taken for testing. A third sibling, a 15−year old girl, is being treated at Hasan Sadikin hospital in Bandung, West Java's provincial capital. Tests for her have been negative. "He died because of breathing problems which he had suffered since he was admitted to the hospital," said Hadi Yusuf, who heads the bird flu ward at Hasan Sadikin hospital. The government said earlier this week the 20−year−old man had bird flu after a series of positive tests for the H5N1 avian flu virus. Yusuf said the brothers had contact with chickens and it was highly unlikely that one infected the other.
Source: http://www.boston.com/news/world/asia/articles/2006/09/28/indonesia_man_dies_of_bird_flu_cluster_case_unlikely/

21. *September 27, Reuters* — **New case of bird flu detected in Egypt.** Another case of avian flu in birds has been confirmed in Egypt. Ministry of Health officials and World Health Organization (WHO) staff said on Wednesday, September 27, that a case of H5N1 (avian flu) in birds was detected in a house near Aswan, in Upper Egypt. WHO spokesperson Hassan el−Bushra said that the infected animals, raised in the backyard of a house in the town of Edfu, have now been culled. This year, Egypt suffered the worst outbreak of avian flu outside Asia. Specialists say that the overwhelming majority of human cases in Egypt have been women who were infected by domestically kept birds.

Source: http://www.alertnet.org/thenews/newsdesk/IRIN/7c76187f30397eded7b2ed740a6199e6.htm

22. *September 27, Clinical Infectious Diseases* — **Safety and immunogenicity of nonadjuvanted and MF59−adjuvanted influenza A/H9N2 vaccine preparations.** Abstract: Influenza A/H9N2 viruses can infect humans and are considered to be a pandemic threat. Effective vaccines are needed for these and other avian influenza viruses. Researchers performed a randomized, double−blind trial to evaluate the safety and immunogenicity of a two−dose schedule of four dose levels of inactivated influenza A/H9N2 vaccine with and without MF59 adjuvant. Vaccine safety was assessed with a diary and selected blood tests. Immunogenicity was measured using serum hemagglutination inhibition (HAI) and microneutralization (MNt) antibody assays. The combination of MF59 adjuvant with a subunit vaccine was associated with improved immune responses to an influenza A/H9N2 virus. The adjuvanted vaccine was immunogenic even after a single dose, raising the possibility that a one−dose vaccination strategy may be attainable with the use of adjuvanted vaccine.
Source: http://www.journals.uchicago.edu/ucp/WebIntegrationServlet?call=ContentWeblet&url=http://www.journals.uchicago.edu/CID/journal/issues/v43n9/39957/39957.html?erFrom=7872203500663860038Guest&current_page=content

23. *September 27, Centers for Disease Control and Prevention* — **Almost half of hospitals experience crowded emergency departments.** Between 40 and 50 percent of U.S. hospitals experience crowded conditions in the emergency department (ED) with almost two−thirds of metropolitan EDs experiencing crowding at times, according to a new report issued Wednesday, September 27, by the Centers for Disease Control and Prevention's (CDC) National Center for Health Statistics. The report, entitled “Staffing, Capacity, and Ambulance Diversion in Emergency Departments: United States, 2003−04,” contains a number of findings, including: An average of 4,500 EDs were in operation in U.S. during 2003 and 2004. Crowding in metropolitan EDs was associated with a higher percentage of nursing vacancies, higher patient volume, and longer patient waiting and treatment durations. Over half the EDs saw fewer than 20,000 patients annually but one out of 10 had an annual visit volume of more than 50,000 patients. Half of EDs in metropolitan areas had more than five percent of their nursing positions vacant. Approximately one−third of U.S. hospitals reported having to divert an ambulance to another emergency department due to overcrowding or staffing shortages at their ED.
Report: http://www.cdc.gov/nchs/data/ad/ad376.pdf
Source: http://www.cdc.gov/od/oc/media/pressrel/r060927.htm

[Return to top]

Government Sector

24. *September 28, Reuters* — **Homeless man named as Colorado school gunman.** The gunman who took students hostage at a high school in Bailey, CO, and killed a girl was 53 and lived out of his car, police said on Thursday, September 28. The gunman, who shot the girl, then himself, as police stormed the classroom on Wednesday, was named as Duane Morrison of Denver by Park County Sheriff Fred Wegener. The sheriff said the motive remained a mystery. Two

weapons−−a revolver and a semi−automatic pistol−−were found on Morrisonies removed his body early on Thursday, Wegener said. The shooting drew comparisons to the 1999 Columbine killings that took place 30 miles away in Littleton, Colorado. At Columbine High School, two students shot and killed 13 people and wounded 21, then committed suicide. Morrison initially took six girls hostage and released all but two. Wegener said he decided to storm the classroom at Platte Canyon High School after Morrison set a deadline and warned "something would happen." Morrison had no known connections with the area, and a "very minor" criminal record, he said.
Source: http://today.reuters.com/news/articlenews.aspx?type=topNews&storyID=2006−09−28T163140Z_01_N27413845_RTRUKOC_0_US−CRIME−COLORADO.xml

25. *September 27, Government Accountability Office* — **GAO−06−1013: Hurricanes Katrina and Rita: Unprecedented Challenges Exposed the Individuals and Households Program to Fraud and Abuse; Actions Needed to Reduce Such Problems in Future (Report).** In 2005, Hurricanes Katrina and Rita caused unprecedented damage. FEMA's Individuals and Households Program (IHP), provides direct assistance (temporary housing units) and financial assistance (grant funding for temporary housing and other disaster−related needs) to eligible individuals affected by disasters. Our objectives were to (1) compare the types and amounts of IHP assistance provided to Hurricanes Katrina and Rita victims to other recent hurricanes, (2) describe the challenges FEMA faced by the magnitude of the requests for assistance following Hurricanes Katrina and Rita, and (3) determine the vulnerability of the IHP program to fraud and abuse. GAO determined the extent to which the program was vulnerability to fraud and abuse, by conducting statistical sampling, data mining and undercover operations. GAO is recommending that FEMA address the potential for fraud and abuse in the IHP by ensuring that payments go to recipients at valid addresses; establishing procedures to avoid duplicate lodging payments; increasing accountability over debit cards; and identifying and recouping payments based on improper and potentially fraudulent applications. FEMA substantially agreed with our recommendations; however DHS disagreed with our estimate of the extent of improper and potentially fraudulent payments.
Highlights: http://www.gao.gov/highlights/d061013high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−1013

[Return to top]

Emergency Services Sector

26. *September 28, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** Tropical Weather Outlook: Atlantic/Gulf of Mexico/Caribbean Sea: At 11:00 p.m. EDT, Wednesday, September 27, Tropical Depression 9 was located about 745 miles east−southeast of Bermuda. Maximum sustained winds are near 35 mph. Some strengthening is forecast and the depression could become a tropical storm. Tropical Depression 9 is moving toward the northwest near 13 mph and this general motion is expected to continue during the next 24 hours. Tropical Depression 9 is not a threat to the U.S. or U.S. territories. Earthquake Activity: A magnitude 6.7 (strong) earthquake occurred 120 miles east−southeast of Hihifo, Tonga; 180 miles south−southwest of Pago Pago, American Samoa at 2:22 a.m. EDT Thursday, September 28. There have been no reports of damage.

To view other Situation Updates: http://www.fema.gov/emergency/reports/index.shtm
Source: http://www.fema.gov/emergency/reports/2006/nat092806.shtm

27. *September 27, Examiner (CO)* — **San Francisco emergency agency's hierarchy clarified following audit.** Following six months of sharp criticism of the San Francisco's emergency planning department, the Board of Supervisors on Tuesday, September 26, unanimously approved legislation that clarifies the department's chain of command and establishes qualifications for the top three emergency heads. The legislation is the latest move by city officials to rectify deficiencies revealed in a city audit of the Office of Emergency Services and Homeland Security (OESHS), including the lack of a comprehensive emergency plan in the event of a major disaster and a lack of experience of OESHS director Annemarie Conroy. The legislation solidifies Laura Phillips as the leader of the city's emergency preparedness functions, changes Conroy's title to deputy director and establishes a deputy director position to oversee emergency communications. It also sets job qualifications for these three posts, ensuring they have past emergency−related job experience.
Source: http://www.examiner.com/a−313259~Agency_s_hierarchy_clarifie d.html

[Return to top]

Information Technology and Telecommunications Sector

28. *September 28, VNUNet* — **U.S. experts launch VoIP security partnership.** A group of U.S. academics and industry experts has been created to explore security issues surrounding Voice over Internet Protocol (VoIP) technology, it was announced Thursday, September 28. The collaboration sees Georgia Tech Information Security Center partnering with BellSouth and Internet Security Systems. The researchers plan to conduct a security analysis of VoIP protocols and implementations, and explore issues such as VoIP authentication for dealing with voice spam, modeling of VoIP traffic and device behavior, mobile phone security, and security of VoIP applications running on user agents.
Source: http://www.vnunet.com/vnunet/news/2165200/experts−launch−voi p−security

29. *September 27, U.S. Computer Emergency Readiness Team* — **Technical Cyber Security Alert TA06−270A: Microsoft Internet Explorer WebViewFolderIcon ActiveX vulnerability.** The Microsoft Windows WebViewFolderIcon ActiveX control contains an integer overflow vulnerability that could allow a remote attacker to execute arbitrary code. Systems Affected: Microsoft Windows and Microsoft Internet Explorer. Exploit code for this vulnerability is publicly available. More information is available in US−CERT Vulnerability Note VU#753044: http://www.kb.cert.org/vuls/id/753044
Solution: Microsoft has not released an update for this vulnerability. Consider the following workarounds and best practices:
Disable the WebViewFolderIcon ActiveX control: To protect against this specific vulnerability, disable the WebViewFolderIcon control by setting the kill bit for the following CLSID: {844F4806−E8A8−11d2−9652−00C04FC30871}. More information about how to set the kill bit is available in Microsoft Support Document 240797:
http://support.microsoft.com/kb/240797
Disable ActiveX: To protect against this and other ActiveX and COM vulnerabilities, disable ActiveX in the Internet Zone and any other zone that might be used by an attacker. Instructions

for disabling ActiveX in the Internet Zone can be found in the "Securing Your Web Browser" document: http://www.us−cert.gov/reading_room/securing_browser/#Intern et_Explorer
Instructions for this can also be found in the Malicious Web Scripts FAQ: http://www.cert.org/tech_tips/malicious_code_FAQ.html#ie56
Render e−mail as plain text: To protect against this and other vulnerabilities that require a victim to load a malicious HTML document, configure e−mail clients to render e−mail as plain text.
Source: http://www.uscert.gov/cas/techalerts/TA06−270A.html

30. *September 27, Security Focus* — **Microsoft PowerPoint unspecified remote code execution vulnerability.** Microsoft PowerPoint is prone to an unspecified remote code execution vulnerability. This issue can allow remote attackers to execute arbitrary code on a vulnerable computer by supplying a malicious PowerPoint document to a user. This issue is being actively exploited in the wild as Trojan.PPDropper.F. This vulnerability is currently known to affect Microsoft Office 2000, Office XP and Office 2003. For a complete list of vulnerable products: http://www.securityfocus.com/bid/20226/info
Due to a lack of information, further details cannot be provided.
Solution: Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/20226/references

31. *September 27, Security Focus* — **Mozilla Firefox/Thunderbird/SeaMonkey multiple remote vulnerabilities.** The Mozilla Foundation has released six security advisories specifying vulnerabilities in Mozilla Firefox, SeaMonkey, and Thunderbird. These vulnerabilities allow attackers to: execute arbitrary code; perform cross−site scripting attacks; supply malicious data through updates; inject arbitrary content; execute arbitrary JavaScript; crash affected applications and potentially execute arbitrary code. Other attacks may also be possible. These issues are fixed in: Mozilla Firefox version 1.5.0.7; Mozilla Thunderbird version 1.5.0.7; Mozilla SeaMonkey version 1.0.5.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/20042/info
Solution: New versions of Firefox, SeaMonkey, and Thunderbird are available to address these issues. Most Mozilla applications have self−updating features that may be used to download and install fixes. Please see the referenced advisories for information on obtaining and applying fixes: http://www.securityfocus.com/bid/20042/references
Source: http://www.securityfocus.com/bid/20042/discuss

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 4672 (eMule), 4662 (eDonkey2000), 445 (microsoft−ds), 113 (auth), 135 (epmap), 139 (netbios−ssn), 6881 (bittorrent), 5900 (vnc), 80 (www) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

32. *September 28, Government Accountability Office* — **GAO−06−1096T: Assessment of the National Capital Region Strategic Plan (Testimony).** The Office of National Capital Region Coordination is to coordinate efforts within the National Capital Region (NCR) to ensure execution of domestic preparedness activities. In the Government Accountability Office's (GAO) May 2004 report and June 2004 testimony before the House Government Reform Committee, GAO recommended that the NCR develop a strategic plan to establish and monitor the achievement of regional goals and priorities for emergency preparedness and response. GAO subsequently testified on the status of the NCR's strategic planning efforts before the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia in July 2005 and March 2006. The Subcommittee asked GAO to provide comments on the NCR's strategic plan, which the NCR partners approved in September 2006. In this testimony, GAO discusses its assessment of the recently completed NCR homeland security strategic plan and the extent to which the new plan includes desirable strategic plan characteristics and how the substance of the plan might be further strengthened when the plan is reviewed and possibly revised. GAO includes no new recommendations in this testimony.
Highlights: http://www.gao.gov/highlights/d061096thigh.pdf
Source: http://www.gao.gov/docsearch/repandtest.html

33. *September 27, NBC 7 (CA)* — **Neighbors rattled by series of pipe−bomb explosions.** Neighbors in one San Diego, CA, neighborhood are on edge, not sure if they have a prankster in their midst or if somebody is actually trying to hurt them. Police said that someone put a pipe bomb near a garage door in Dennison late Saturday night, September 23. The four people inside the home were not hurt by the blast, which ripped a hole in the garage door. Investigators said another pipe bomb blew up two months ago a few blocks away on Streseman Street. That explosion destroyed a U.S. Postal Service mailbox, which has since been replaced. Investigators were not sure if the two bombings are connected, but they did say that the devices were very similar. Investigators have not yet found any evidence linking the bombs to anybody.
Source: http://www.nbcsandiego.com/news/9947528/detail.html

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer